

ELECTRONIC CONFERENCE SYSTEM, ELECTRONIC CONFERENCE METHOD, PROGRAM, AND STORAGE MEDIUM

Publication number: JP2003304518 (A)

Publication date: 2003-10-24

Inventor(s): NAGO HIDETADA +

Applicant(s): CANON KK +

Classification:

- **international:** *H04N7/15; H04L12/28; H04M3/56; H04N7/15; H04L12/28; H04M3/56; (IPC1-7): H04N7/15; H04L12/28; H04M3/56*

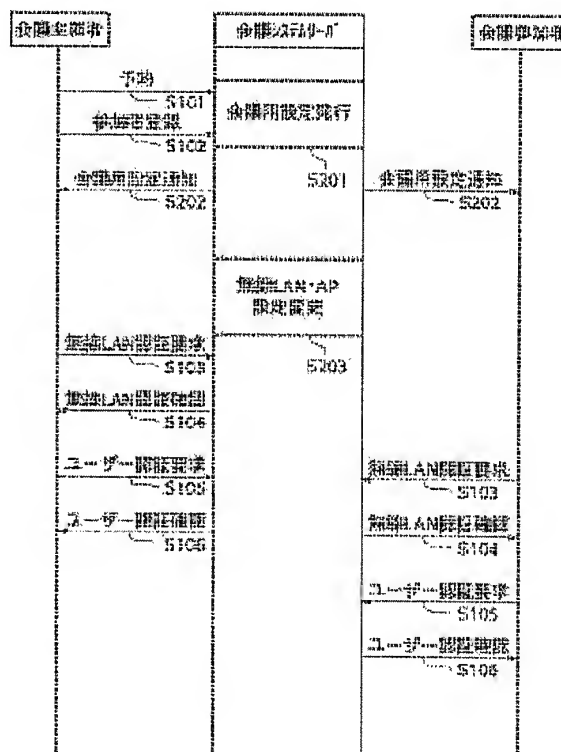
- **European:**

Application number: JP20020109364 20020411

Priority number(s): JP20020109364 20020411

Abstract of JP 2003304518 (A)

PROBLEM TO BE SOLVED: To provide an electronic conference system in which participants can take participation without the need for a special work and which can prevent a malicious act by a third party such as interception of contents of the conference. ; **SOLUTION:** A conference sponsor makes a reservation for a conference at a conference system server 2 (S101) and registers electronic mail addresses of conference participants (S102). The conference system server 2 issues conference purpose setting information such as accounts and passwords different from the participants (S201), and transmits electronic mail describing the contents of the information to the conference sponsor and the conference participants (S202). Each participant starts a conference system installed on its own terminal 4 and allows the conference system to read the conference purpose setting information described in the notified electronic mail to take participation in the conference. ; **COPYRIGHT:** (C)2004,JPO



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-304518

(P2003-304518A)

(43) 公開日 平成15年10月24日 (2003. 10. 24)

(51) Int.Cl. ⁷	識別記号	F I	データベース* (参考)
H 0 4 N 7/15	6 5 0	H 0 4 N 7/15	6 5 0 5 C 0 6 4
H 0 4 L 12/28	3 0 0	H 0 4 L 12/28	3 0 0 Z 5 K 0 1 5
H 0 4 M 3/56		H 0 4 M 3/56	C 5 K 0 3 3

審査請求 未請求 請求項の数12 O L (全 13 頁)

(21) 出願番号 特願2002-109364(P2002-109364)

(22) 出願日 平成14年4月11日 (2002. 4. 11)

(71) 出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

(72) 発明者 名合 秀忠

東京都大田区下丸子3丁目30番2号 キヤ
ノン株式会社内

(74) 代理人 100081880

弁理士 渡部 敏彦

Fターム(参考) 5C064 AA02 AC02 AC06 AC12 AC16

AC18 AC22

5K015 AA10 AB01 AF06 JA02

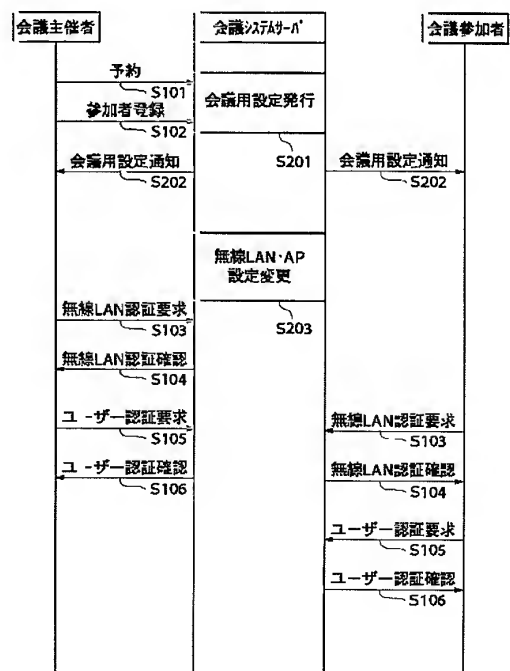
5K033 AA08 DA17

(54) 【発明の名称】 電子会議システム、電子会議方法、プログラムおよび記憶媒体

(57) 【要約】

【課題】 参加者が特別な作業を行うことなく会議に参加でき、しかも、第三者による会議内容の盗聴といった悪意ある行為を防止できる電子会議システムを提供する。

【解決手段】 会議主催者は、会議システムサーバ2に会議の予約を行い (S101)、会議参加者の電子メールアドレスを登録する (S102)。会議システムサーバ2は参加者毎に異なるアカウントおよびパスワード等の会議用設定情報を発行し (S201)、その内容を記載した電子メールを送る (S202)。参加者は、所有する端末4に搭載されている会議システムを起動させ、通知された電子メールに記載されている会議設定情報を読み込ませることで、会議に参加する。



【特許請求の範囲】

【請求項1】 ネットワークを介して会議サーバおよびクライアントが接続され、電子データを共有することで会議を行う電子会議システムにおいて、会議の予約を行い、この会議への参加者を登録する登録手段と、前記登録された参加者にそれぞれ固有の識別情報を発行する発行手段と、前記発行した識別情報を前記登録された参加者が所有する端末に通知する通知手段と、前記ネットワークに接続された端末が前記クライアントとして起動した場合、前記通知された識別情報を取得する取得手段と、前記クライアントの識別情報の認証を前記会議サーバに要求する要求手段と、前記認証を要求された識別情報が有効であるか否かを判断する判断手段と、前記識別情報が有効である場合、前記クライアントに会議への参加を許可する許可手段とを備えたことを特徴とする電子会議システム。

【請求項2】 前記会議サーバと有線ネットワークを介して通信可能であり、前記クライアントと無線ネットワークを介して通信可能である無線通信装置を備え、前記通知手段は、前記識別情報とともに、前記無線通信装置と無線通信を行うための通信設定情報を通知し、前記端末は、前記通知された通信設定情報を基に、前記無線通信装置と無線通信を行うための設定を変更することを特徴とする請求項1記載の電子会議システム。

【請求項3】 前記会議サーバは、前記クライアントと無線ネットワークを介して無線通信を行う無線通信手段、前記登録手段、前記発行手段および前記通知手段を備え、前記無線通信を行うための通信設定情報を決定し、前記識別情報とともに、前記決定された通信設定情報を通知し、前記クライアントは、前記取得手段を備え、前記会議サーバから通知された通信設定情報を前記識別情報と共に取得し、該取得した通信設定情報を基に、前記会議サーバとの無線通信を確立することを特徴とする請求項1記載の電子会議システム。

【請求項4】 前記会議サーバとは別のネットワーク上に設けられた予約サーバは、前記登録手段、前記発行手段および前記通知手段を備え、前記会議サーバと無線通信を行うための通信設定情報を決定し、該決定した通信設定情報および前記識別情報を通知するとともに、前記通信設定情報を着脱式の記録媒体に記憶しておき、前記会議サーバは、前記クライアントと無線ネットワークを介して無線通信を行う無線通信手段を備え、前記記録媒体に記憶された通信設定情報を基に、前記無線通信を行うための設定を変更し、前記クライアントは、前記取得手段を備え、前記予約サ

ーバから通知された通信設定情報を前記識別情報と共に取得し、該取得した通信設定情報を基に、前記会議サーバとの無線通信を確立することを特徴とする請求項1記載の電子会議システム。

【請求項5】 前記会議サーバは、前記クライアントと無線ネットワークを介して無線通信を行う無線通信手段、前記登録手段、前記発行手段および前記通知手段を備え、前記無線ネットワークとは別のネットワークに接続された状態で、前記会議の予約を行い、この会議への参加者を登録し、該会議サーバと無線通信を行うための通信設定情報を決定し、該決定した通信設定情報および前記識別情報を通知するとともに、前記無線通信を行うための設定を変更し、

前記クライアントは、前記取得手段を備え、前記会議サーバから通知された通信設定情報を前記識別情報と共に取得し、該取得した通信設定情報を基に、前記会議サーバとの無線通信を確立することを特徴とする請求項1記載の電子会議システム。

【請求項6】 前記登録手段は、前記参加者の電子メールアドレスを登録し、前記通知手段は前記登録された電子メールアドレス宛に電子メールで通知することを特徴とする請求項1乃至5のいずれかに記載の電子会議システム。

【請求項7】 全ての参加者のログアウト処理が行われると、会議終了とみなし、所定時間内に次の会議の予定がある場合、前記無線通信装置の設定を次の会議用のものに変更する一方、前記所定時間内に次の会議の予定がない場合、ランダムに生成された通信設定情報を基に、前記無線通信装置の設定を変更することを特徴とする請求項2記載の電子会議システム。

【請求項8】 全ての参加者のログアウト処理が行われると、会議の終了とみなし、前記無線通信手段の電源をオフにするか、あるいは前記会議サーバの全電源をオフにすることを特徴とする請求項3乃至5のいずれかに記載の電子会議システム。

【請求項9】 前記会議サーバは、前記判断手段を備え、前記認証を要求された識別情報と同一の識別情報を有する参加者が既に存在する場合、その旨の警告を参加者に送信することを特徴とする請求項1乃至8のいずれかに記載の電子会議システム。

【請求項10】 ネットワークを介して会議サーバおよびクライアントが接続され、電子データを共有することで会議を行う電子会議方法において、会議の予約を行い、この会議への参加者を登録するステップと、前記登録された参加者にそれぞれ固有の識別情報を発行するステップと、前記発行した識別情報を前記登録された参加者が所有する端末に通知するステップと、

前記ネットワークに接続された端末が前記クライアントとして起動した場合、前記通知された識別情報を取得するステップと、
前記クライアントの識別情報の認証を前記会議サーバに要求するステップと、
前記認証を要求された識別情報が有効であるか否かを判断するステップと、
前記識別情報が有効である場合、前記クライアントに会議への参加を許可するステップとを有することを特徴とする電子会議方法。

【請求項11】 請求項10に記載の電子会議方法を実現するためのコンピュータ読み取り可能なプログラムコードを保持する記憶媒体。

【請求項12】 請求項10に記載の電子会議方法を實現するためのコンピュータ読み取り可能なプログラムコードを有するプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、会議室において、電子データを共有して会議を行う電子会議システム、電子会議方法、プログラムおよび記憶媒体に関する。

【0002】

【従来の技術】従来、会議は、一般的に資料となる書類を配布して進められる。しかし、近年、書類の代わりに、電子データをやり取りし、資料を電子的に改変しながら進める電子会議システムが知られている。例えば、特開平09-081489号公報に示される有線ネットワークによる電子会議システムでは、会議に参加できない場合でも、その参加できない人の資料だけは会議で使えるようにすることが提案されている。

【0003】

【発明が解決しようとする課題】しかしながら、従来の電子会議システムでは、以下に掲げる問題があり、その改善が要望されていた。コンピュータ等の端末を会議室に持ち込み、その端末を有線LANに接続して会議を行う場合、IPアドレスなどのネットワークの設定を変更する必要があったり、LANケーブルを会議室内に引き回すといった煩わしさがあった。

【0004】こういう煩わしさを解消するために、会議用サーバと、会議に参加する人の端末との間で無線通信を採用する方式が提案されている。一般的には、IEEE802.11で規定された無線LANが用いられている。

【0005】しかし、無線は広がりを持ったある範囲に伝播するので、特定の相手のみに送ることができず、悪意のある第三者の盗聴を受けるおそれがあった。また、悪意のある第三者に無線の設定が知られると、ネットワークに侵入されるという無線特有の問題が生じるおそれがあった。

【0006】上記特開平09-081489号公報の電

子会議システムでは、有線ネットワークを前提としており、無線化によるセキュリティの脆弱性は考慮されていなかった。また、グループ全員が同一内容のグループリストを有し、グループリストを基に暗号化鍵を生成する方法が提案されている。会議のように、メンバーが会議毎に入れ替わるような場合、あまり使い易い方法とはいえなかった。

【0007】また、特開平05-48746号公報の電子会議システムでは、会議毎にコード番号を発行し、会議参加時にコード番号を入力するといった方法が提案されている。しかし、無線化した場合、覚え易い短めのコードだと容易に第三者に知られ、会議内容のセキュリティを確保することが難しかった。さらに、有線と同様、ネットワークの設定など、各種の設定が必要であった。

【0008】そこで、本発明は、参加者が特別な作業を行うことなく会議に参加でき、しかも、第三者による会議内容の盗聴といった悪意ある行為を防止できる電子会議システム、電子会議方法、プログラムおよび記憶媒体を提供することを目的とする。

【0009】

【課題を解決するための手段】上記目的を達成するために、本発明の電子会議システムは、ネットワークを介して会議サーバおよびクライアントが接続され、電子データを共有することで会議を行う電子会議システムにおいて、会議の予約を行い、この会議への参加者を登録する登録手段と、前記登録された参加者にそれぞれ固有の識別情報を発行する発行手段と、前記発行した識別情報を前記登録された参加者が所有する端末に通知する通知手段と、前記ネットワークに接続された端末が前記クライアントとして起動した場合、前記通知された識別情報を取得する取得手段と、前記クライアントの識別情報の認証を前記会議サーバに要求する要求手段と、前記認証を要求された識別情報が有効であるか否かを判断する判断手段と、前記識別情報が有効である場合、前記クライアントに会議への参加を許可する許可手段とを備えたことを特徴とする。

【0010】本発明の電子会議方法は、ネットワークを介して会議サーバおよびクライアントが接続され、電子データを共有することで会議を行う電子会議方法において、会議の予約を行い、この会議への参加者を登録するステップと、前記登録された参加者にそれぞれ固有の識別情報を発行するステップと、前記発行した識別情報を前記登録された参加者が所有する端末に通知するステップと、前記ネットワークに接続された端末が前記クライアントとして起動した場合、前記通知された識別情報を取得するステップと、前記クライアントの識別情報の認証を前記会議サーバに要求するステップと、前記認証を要求された識別情報が有効であるか否かを判断するステップと、前記識別情報が有効である場合、前記クライアントに会議への参加を許可するステップとを有することを

特徴とする。

【0011】

【発明の実施の形態】本発明の電子会議システム、電子会議方法、プログラムおよび記憶媒体の実施の形態について、図面を参照しながら説明する。

【0012】〔第1の実施形態〕図1は第1の実施形態における電子会議システムの構成を示す図である。図において、1は無線LANアクセスポイントである。2は会議システムサーバである。3は有線LANである。4は会議で使用する端末である。

【0013】図2は会議の予約から会議開始時までの動作処理手順を示すフローチャートである。本実施形態では、無線通信方式にIEEE802.11で規定されている無線LANを用いる場合を示す。

【0014】会議室には、通常の無線LANアクセスポイント（AP）1が存在し、会議システムを運営するサーバ2は別の場所に存在する。ここでは、このサーバ2を会議システムサーバ2と称する。AP1および会議システムサーバ2は、有線LAN3で接続されている。

【0015】会議システムサーバ2は会議予約機能を有し、会議の主催者は、会議システムサーバ2上で会議を予約する（S101）。この予約の際、会議の日時、会議室、参加者のメールアドレスを登録する（S102）。

【0016】会議システムサーバ2は、会議の予約を受け付けると、会議に必要な無線LANの無線グループIDおよび無線LAN用暗号化キーを決定し、さらに、予約された会議だけで有効なアカウントおよびパスワードを参加者分だけ発行する（201）。そして、登録されたメールアドレスを基に、これらの情報を電子メール内に記載し、各参加者にその電子メールを送る（S202）。

【0017】このように、会議参加者宛ての電子メールには、会議の日時、会議で使用する無線グループID、無線LAN用暗号化キー、1人分のアカウントおよび1人分のパスワードが記載されている。電子メールに記載されたこれらの会議用設定情報は、通常のテキストデータであってもよいが、会議システム（ソフトウェア）同士でのみ有効な符号に置き換えておくことが望ましい。会議システムサーバ2は、会議予約情報に、会議で使用する無線グループID、無線LAN用暗号化キー、全ての参加者のアカウントおよびアカウントに対応するパスワードを記録する。

【0018】各会議参加者は、会議システムサーバ2から送られてきた電子メールを会議で使用する端末4に渡し、端末4内の会議システム（ソフトウェア）を起動させて、会議システムサーバ2から送られてきた電子メールを読み込ませる。会議システムは、読み込んだ電子メールから会議の日時、会議で使用する無線グループID、無線LAN用暗号化キー、1人分のアカウントおよ

び1人分のパスワードを取り出して記憶する。

【0019】複数の会議を管理するために、図3に示すような会議スケジュール管理を行う。図3は会議スケジュール管理を示す図である。会議参加者は、会議の日時と場所の情報だけを知り、会議の無線通信の設定情報やアカウントおよびパスワードについては、会議システムが管理するので、知らなくてよい。また、第三者の目に触れないためにも、会議参加者の目に触れさせない方が望ましい。

【0020】会議を予約した時間になると、会議システムサーバ2は、会議で使用する無線LANアクセスポイント1内の無線グループIDおよび無線LAN用暗号化キーの設定を変更する（S203）。

【0021】参加者は、会議システム（ソフトウェア）が搭載されている端末4を会議室に持ち込み、端末4を立ち上げ、会議システムを起動する。起動した会議システムは、予め読み込んだ電子メールに記載されていた会議で使用する無線グループIDおよび無線LAN用暗号化キーを端末4に接続されている無線LANカードに設定する。端末4が無線LANを内蔵している場合、内蔵無線LANに設定する。

【0022】会議システムは、無線LANの接続要求（無線LAN認証要求、S103）および接続完了後（無線LAN認証確認、S104）、無線LANを経由して同じ電子メールに記載されていたアカウントで会議システムサーバ2にログインし（ユーザ認証要求、S105）、パスワードで認証する（ユーザ認証確認、S106）。

【0023】会議システムサーバ2は、アカウント名およびパスワードを参照し、有効なアカウント名である場合、会議に参加させる。ここで、会議に代理人を出席させる場合、会議システムサーバ2から送られてきた電子メールを、転送するかあるいは記録媒体に記録して代理人に渡す。そして、代理人は会議に持ち込む端末4に搭載されている会議システムを起動させ、会議システムサーバ2から送られてきた電子メールを読み込ませる。出席者が変わっても、会議用のアカウントのみで有効な出席者であるか否かを判断するので、容易に代理人を出席させることが可能となる。

【0024】同一のアカウントのログインが発生した場合、一方が不正なログインをしているおそれがある。これを検出するために、会議システムサーバ2は、会議が始まると、アカウントのログイン処理を行う。図4はアカウントのログイン処理手順を示すフローチャートである。この処理プログラムは、会議システムサーバ2内の記憶媒体に格納されており、会議システムサーバ2内のCPUによって実行される。

【0025】まず、ログイン要求があるまで待ち（ステップS1）、ログイン要求があると、同一ログインフラグを調べる（ステップS2）。同一ログインフラグが立

っていない(セットされていない)場合、今回ログイン要求されたアカウントと同じアカウントからのログイン要求が既にあったか否かを調べる(ステップS3)。同じアカウントからのログイン要求がなかった場合、正常なログイン処理を行い(ステップS4)、ステップS1の処理に戻り、次のログイン要求を待つ。

【0026】一方、ステップS3で同一のアカウントからのログイン要求が既にあった場合、同一のアカウントからのログイン要求があったことを示す同一ログインフラグをセットし(ステップS5)、既にログインしている会議出席者の有無を調べる(ステップS6)。会議出席者がいない場合、ステップS1の処理に戻って、次のログイン要求を待つ。一方、既に会議出席者がいる場合、正常にログインした出席者に不正なログインがあった旨の警告を送信する(ステップS7)。この後、ステップS1の処理に戻る。

【0027】そして、ステップS5で同一ログインフラグがセットされると、次にログイン要求があった場合、ステップS2における同一ログインフラグのチェックの結果、この会議には不正なログイン処理が行われている旨の警告を表示し(ステップS8)、ステップS1の処理に戻る。

【0028】そして、不正なログインがあると、会議システムサーバ2は、会議主催者だけにアクセスを許可する。不正なログインの警告を目にした会議主催者は、会議システムサーバ2に会議用設定情報の再発行を依頼する。依頼を受けた会議システムサーバ2は、会議用設定情報を新たに決定し、その設定ファイルを会議主催者に渡す。渡された設定ファイルには、新しい無線グループID、無線LAN用暗号化キー、この会議に共通のアカウントおよびパスワードが記載されている。主催者は、記録媒体を使用するか、あるいは無線LANの1対1通信モードを使用して、他の参加者に新しい会議用設定情報を通知する。不正ログインを行った第三者が、この時点で新たな会議用設定情報を知ることは不可能であるので、会議内容を知ることはできない。会議システムサーバ2は、念のため、参加者のログイン数を調べ、予約時に登録されているメールアドレスの数とこのログイン数の比較を行う。

【0029】尚、電子メールそのものに、会議の日時、会議で使用する無線グループID、無線LAN用暗号化キー、1人分のアカウントおよび1人分のパスワードからなる会議用設定情報を記載する代わりに、電子メールにファイルを添付してもよく、この添付ファイルに会議の日時、会議で使用する無線グループID、無線LAN用暗号化キー、1人分のアカウントおよび1人分のパスワードを記載しておくことでも、同様の動作が実現可能である。

【0030】また、全ての出席者のログアウト処理が行われると、会議システムサーバ2は、会議終了であると

判断し、会議終了であると判断した会議用のアカウントおよびパスワードを破棄する。また、無線LANアクセスポイント1の設定を次の会議用のものに変更する。ここで、次の会議の予定がない場合、あるいは次の会議まで長時間ある場合、ランダムに生成した無線グループIDおよび無線LAN用暗号化キーでその設定を変更し、悪意の第三者の不正アクセスを防止する。

【0031】このように、本実施形態では、会議予約時に発行する電子メールに、会議の日時、会議で使用する無線グループID、無線LAN用暗号化キー、1人分のアカウントおよび1人分のパスワードを記載し、参加者の端末に搭載されている会議システムに読み込ませるだけで、自動的に会議に参加でき、しかも第三者による会議内容の盗聴といった悪意ある行為を防止することができ。

【0032】[第2の実施形態]図5は第2の実施形態における電子会議システムの構成を示す図である。前記第1の実施形態と同様の構成要素については、同一の符号を付すことにする。図において、3は有線LANである。4は会議で使用する端末である。5は多機能アクセスポイントである。

【0033】図6は多機能アクセスポイントの内部構成を示すブロック図である。図において、51は制御部である。52は無線LANアクセスポイント部である。53は不揮発性記憶部である。54は着脱式記憶部である。55は有線LANインターフェイスである。無線LANアクセスポイント部52は、大人数で会議を行う際、トラフィックの分散を図るため、複数存在することもある。

【0034】また、会議の予約から会議開始時の処理、および同一のアカウントのログインがあった場合の処理は、前記第1の実施形態における図2および図4と同様である。

【0035】多機能無線LANアクセスポイント(MFAP)5は会議室に設けられており、有線LAN3に接続され、有線LAN3側から会議の予約などが行うことが可能である。MFAP5では、会議の予約機能を有した会議システム(ソフトウェア)が動作しており、MFAP5は無線LANアクセスポイントとしての機能の他、無線LAN側と有線LAN3側へのアクセスを可能にする機能を有する。したがって、図2における会議システムサーバの機能はMFAP5によって実現されている。

【0036】会議主催者は、希望する会議室に設置されているMFAP5で会議の予約を行う(S101)。予約の際、会議の日時、参加者のメールアドレスを登録する(S102)。会議の予約を受け付けると、MFAP5は、会議に必要な無線LANの無線グループIDおよび無線LAN用暗号化キーを決定し、さらに、予約された会議だけで有効なアカウントおよびパスワードを参加

者分だけ発行する（S201）。

【0037】登録されたメールアドレスを基に、これらの情報を電子メール内に記載し、各参加者に電子メールを送る（S202）。参加者宛ての電子メールには、会議の日時、会議で使用する無線グループID、無線LAN用暗号化キー、1人分のアカウントおよび1人分のパスワードが記載されている。電子メールに記載されたこれらの会議用設定情報は、通常のテキストデータであってもよいが、会議システム（ソフトウェア）同士でのみ有効な符号に置き換えておくことが望ましい。MFAP5は、会議予約の情報に、会議で使用する無線グループID、無線LAN用暗号化キー、全ての参加者のアカウントおよびこれらのアカウントに対応するパスワードを不揮発性記憶部53に記憶する。

【0038】MFAP5が、複数の無線LANアクセスポイント部52を有する場合、各々の無線LANアクセスポイント部52毎に異なる無線グループIDおよび無線LAN用暗号化キーを設定することで、会議時、MFAP5内の無線LANアクセスポイント部52に接続される端末4の数を均等化することができ、無線区間におけるトラフィックの低下を防止できる。この場合、内蔵する無線LANアクセスポイント部52の数分だけ無線グループIDおよび無線LAN用暗号化キーを決定し、内蔵する無線LANアクセスポイント部52に、登録された会議参加者が均等になるように割り当て（S201）、登録されたメールアドレスを基に、これらの情報を電子メール内に記載し、各参加者に電子メールを送る（S202）。この参加者宛ての電子メールには、会議の日時、MFAP5が会議で割り当てた無線LANアクセスポイント部52の設定情報である無線グループID、無線LAN用暗号化キー、会議で使用する1人分のアカウントおよび1人分のパスワードが記載されている。

【0039】各会議参加者は、MFAP5から送られてきた電子メールを会議で使用する端末4に渡し、会議システム（ソフトウェア）を起動させ、MFAP5から送られてきた電子メールを読み込ませる。会議システムは、読み込んだ電子メールから会議の日時、会議で使用する無線グループID、無線LAN用暗号化キー、1人分のアカウントおよび1人分のパスワードを取り出して記憶する。

【0040】複数の会議を管理するために、図3に示すような会議スケジュール管理を行う。会議参加者は、会議の日時および場所の情報だけを知ることができるが、会議の無線通信の設定情報やアカウントおよびパスワードについては、会議システムが管理するので、会議参加者は知らなくてもよい。また、第三者の目に触れさせないためにも、会議参加者の目に触れさせない方が望ましい。

【0041】会議を予約した時間になると、MFAP5

は、会議で使用する無線LANアクセスポイント部52における無線グループIDおよび無線LAN用暗号化キーの設定を不揮発性記憶部53から読み出して変更する（S203）。

【0042】参加者は、会議システム（ソフトウェア）が搭載されている端末4を持ち込み、端末4を立ち上げ、会議システムを起動する。起動した会議システムは、予め読み込んだ電子メールに記載されていた会議で使用する無線グループIDおよび無線LAN用暗号化キーを端末4に接続されている無線LANカードに設定する。端末4が無線LANを内蔵している場合、内蔵無線LANに設定する。

【0043】そして、会議システムは、無線LANの接続要求を行い（無線LAN認証要求、S103）、接続完了後（無線LAN認証確認、S104）、無線LANを経由して同じ電子メールに記載されていたアカウントでMFAP5内部の会議システムにログインし（ユーザ認証要求、S105）、パスワードで認証する（ユーザ認証確認、S106）。

【0044】MFAP5は、アカウント名およびパスワードを参照し、有効なアカウント名である場合、会議に参加させる。会議に代理人を出席させる場合、MFAP5から送られてきた電子メールを転送するか、あるいは記録媒体に記録して代理人に渡す。代理人は、会議に持ち込む端末4に搭載されている会議システムを起動させ、MFAP5から送られてきた電子メールを読み込ませる。出席者は変わっても、会議用のアカウントだけで有効な出席者が否かを判断するので、容易に代理人を出席させることが可能となる。

【0045】また、同一アカウントのログインが発生した場合、前記第1の実施形態と同様、図4に示す処理が行われる。すなわち、同一のアカウントのログインが発生した場合、一方が不正なログインをしているおそれがある。これを検出するために、MFAP5は、会議が始まると、同一のアカウントのログイン処理を行う。

【0046】まず、ログイン要求があるまで待ち（ステップS1）、ログイン要求があると、同一ログインフラグを調べる（ステップS2）。同一ログインフラグが立っていない（セットされていない）場合、今回ログイン要求されたアカウントと同じアカウントからのログイン要求が既にあったか否かを調べる（ステップS3）。同じアカウントからのログイン要求がなかった場合、正常なログイン処理を行い（ステップS4）、ステップS1の処理に戻り、次のログイン要求を待つ。

【0047】一方、ステップS3で同一のアカウントからのログイン要求が既にあった場合、同一のアカウントからのログイン要求があったことを示す同一ログインフラグをセットし（ステップS5）、既にログインしている会議出席者の有無を調べる（ステップS6）。会議出席者がいない場合、ステップS1の処理に戻って、次の

ログイン要求を待つ。一方、既に会議出席者がいる場合、正常にログインした出席者に不正なログインがあった旨の警告を送信する（ステップS7）。その後、ステップS1の処理に戻る。

【0048】そして、ステップS5で同一のログインフラグがセットされると、次にログイン要求があった場合、ステップS2における同一ログインフラグのチェックの結果、この会議には不正なログイン処理が行われている旨の警告を表示し（ステップS8）、ステップS1の処理に戻る。

【0049】そして、不正なログインがあると、MFAP5は、会議主催者だけにアクセスを許可する。不正なログインの警告を目にした会議主催者は、MFAP5に会議用設定情報の再発行を依頼する。依頼を受けたMFAP5は、会議用設定情報を新たに決定し、その設定用ファイルを会議主催者に渡す。渡された設定用ファイルには、新しい無線グループID、無線LAN用暗号化キー、この会議共通のアカウントおよびパスワードが記載されている。主催者は、記録媒体を使用するかあるいは無線LANの1対1通信モードを使用し、他の参加者に新しい会議用設定情報を通知する。不正ログインを行った第三者が、この時点で新たな会議用設定情報を知ることが不可能であるので、会議内容を知ることができない。MFAP5は、念のため、参加者のログイン数を調べ、予約時に登録されているメールアドレスの数とこのログイン数の比較を行う。

【0050】全ての出席者のログアウト処理が行われると、MFAP5は、会議終了と判断し、会議終了と判断した会議用のアカウントおよびパスワードを破棄する。また、無線LANアクセスポイント部52の設定を次の会議用のものに変更する。ここで、次の会議の予定がない場合、あるいは次の会議まで長時間ある場合、ランダムに生成した無線グループIDおよび無線LAN用暗号化キーで設定を変更し、悪意の第三者の不正アクセスを防止する。さらには、長時間に亘って使用されない場合、無線LANアクセスポイント部52あるいは無線LANアクセスポイント5の電源を落とし、不正なアクセスを防止するようにしてもよい。

【0051】尚、電子メールそのものに、会議の日時、会議で使用する無線グループID、無線LAN用暗号化キー、1人分のアカウントおよび1人分のパスワードを記載する代わりに、電子メールにファイルを添付し、この添付ファイルに会議の日時、会議で使用する無線グループID、無線LAN用暗号化キー、1人分のアカウントおよび1人分のパスワードを記載してもよく、同様の動作が実現可能である。

【0052】このように、会議予約時に発行する電子メールに、会議の日時、会議で使用する無線グループID、無線LAN用暗号化キー、1人分のアカウントおよび1人分のパスワードを記載し、参加者の端末に搭載さ

れている会議システムに読み込ませるだけで、自動的に会議に参加でき、しかも第三者による会議内容の盗聴といった悪意ある行為を防止することができる。

【0053】[第3の実施形態] 図7は第3の実施形態における電子会議システムの構成を示す図である。前記第1および第2の実施形態と同一の構成要素は同一の符号で示される。図において、3は有線LANである。4は会議で使用する端末である。5は多機能アクセスポイントである。6は会議予約サーバである。

【0054】多機能アクセスポイントの構成は、図6に示す通り、前記第2の実施形態と同様である。そして、大人数での会議を行った場合、トラフィックの分散を図るために、無線LANアクセスポイント部52は複数存在することもある。

【0055】図8は第3の実施形態における会議の予約から会議開始時までの処理手順を示すフローチャートである。まず、多機能無線LANアクセスポイント(MFAP)5は持ち運び自在であり、有線LAN3から切り離されている。有線LAN3上には、会議用設定情報を作成する会議予約サーバ6が存在している。ここでは、会議予約サーバ6を用いて、会議の予約を行う場合を示す。また、会議システムサーバの機能はMFAP5によって実現されている。

【0056】会議主催者は、会議予約サーバ6で会議の予約を行う(S101)。予約の際、会議の日時および参加者のメールアドレスを登録する(S102)。一方、会議の予約を受け付けると、会議予約サーバ6は、会議に必要な無線LANの無線グループIDおよび無線LAN用暗号化キーを決定し、また、予約された会議だけで有効なアカウントおよびパスワードを参加者分だけ発行する(S201)。そして、登録されたメールアドレスを基に、これらの情報を電子メール内に記載し、各参加者に電子メールを送る(S202)。

【0057】参加者宛ての電子メールには、会議の日時、会議で使用する無線グループID、無線LAN用暗号化キー、1人分のアカウントおよび1人分のパスワードが記載されている。電子メールに記載されたこれらの会議用設定情報は、通常のテキストデータであってもよいが、会議システム(ソフトウェア)同士でのみ有効な符号に置き換えておくことが望ましい。

【0058】会議予約サーバ6は、MFAP5で使用する無線グループID、無線LAN用暗号化キー、全ての参加者のアカウントおよびこのアカウントに対応するパスワードを記録し、会議主催者に電子メールで送る(S204)。ここで、MFAP5が複数の無線LANアクセスポイント部52を有する場合、各無線LANアクセスポイント部52毎に、異なる無線グループIDおよび無線LAN用暗号化キーを設定することで、会議時、MFAP5内の無線LANアクセスポイント部52に接続される端末4の数を均等化することができ、無線区間で

のトラフィックの低下を防止できる。この場合、内蔵する無線LANアクセスポイント部52の数分だけ無線グループIDおよび無線LAN用暗号化キーを決定し、内蔵する無線LANアクセスポイント部52に、登録された会議参加者が均等になるように割り当て(S201)、登録されたメールアドレスを基に、これらの情報を電子メール内に記載して各参加者に電子メールを送信する(S202)。

【0059】参加者宛ての電子メールには、会議の日時、MFAP5が会議で割り当てた無線LANアクセスポイント部52の設定情報である無線グループIDおよび無線LAN用暗号化キー、および会議で使用する1人分のアカウントおよび1人分のパスワードが記載されている。

【0060】各会議参加者は、会議予約サーバ6から送られてきた電子メールを会議で使用する端末4に渡し、会議システムを起動させ、会議予約サーバ6から送られてきた電子メールを読み込ませる。会議システム(ソフトウェア)は、読み込んだ電子メールから会議の日時、会議で使用する無線グループID、無線LAN用暗号化キー、1人分のアカウントおよび1人分のパスワードを取り出して記憶する。また、複数の会議を管理するために、図3に示すような会議スケジュール管理を行う。会議参加者は、会議の日時および場所の情報だけを知ることができるが、会議の無線通信設定情報やアカウントおよびパスワードは、会議システムが管理するので、会議参加者は知らなくてもよい。また、第三者の目に触れないためにも会議参加者の目に触れさせない方が望ましい。

【0061】会議主催者は、会議予約サーバ6から送られてきたMFAP5用の設定データおよび参加者の認証用データをメモ리카ードのような着脱自在な記憶媒体(着脱式記憶部)に記録し、これを会議開始前にMFAP5の着脱式記憶部54に装着し、会議用設定情報をMFAP5に読み込ませる(S205)。MFAP5は、着脱式記憶部54の記録媒体中に記録されている無線グループIDおよび無線LAN用暗号化キーを無線LANアクセスポイント部52に設定する。

【0062】参加者は、会議システムが搭載されている端末4を持ち込み、端末4を立ち上げ、会議システムを起動する。起動した会議システムは、予め読み込んだ電子メールに記載されていた会議で使用する無線グループIDおよび無線LAN用暗号化キーを、端末4に接続されている無線LANカードに設定する。端末4が無線LANを内蔵する場合、内蔵無線LANに設定する。

【0063】会議システムは、無線LANの接続を要求し(無線LAN認証要求、S103)、接続完了後(無線LAN認証確認、S104)、無線LANを経由して同じ電子メールに記載されていたアカウントでMFAP5内部の会議システムにログインし(ユーザ認証要求、

S105)、パスワードで認証する(ユーザ認証確認、S106)。

【0064】MFAP5は、着脱式記憶部54に装着された記憶媒体に記載されたアカウントおよびパスワードを参照し、有効なアカウント名である場合、会議に参加させる。会議に代理人を出席させる場合、MFAP5から送られてきた電子メールを転送するか、あるいは記録媒体に記録して代理人に渡す。代理人は会議に持ち込む端末4に搭載されている会議システムを起動し、会議予約サーバ6から送られてきた電子メールを読み込ませる。出席者は変わっても、会議用のアカウントだけで有効な出席者か否かを判断するので、容易に代理人を出席させることが可能となる。

【0065】また、同一アカウントのログインが発生した場合、前記第1の実施形態と同様、図4に示す処理が行われる。すなわち、同一のアカウントのログインが発生した場合、一方が不正なログインをしているおそれがある。これを検出するために、MFAP5は、会議が始まると、アカウントのログイン処理を行う。

【0066】まず、ログイン要求があるまで待ち(ステップS1)、ログイン要求があると、同一ログインフラグを調べる(ステップS2)。同一ログインフラグが立っていない(セットされていない)場合、今回ログイン要求されたアカウントと同じアカウントからのログイン要求が既にあったか否かを調べる(ステップS3)。同じアカウントからのログイン要求がなかった場合、正常なログイン処理を行い(ステップS4)、ステップS1の処理に戻り、次のログイン要求を待つ。

【0067】一方、ステップS3で同一のアカウントからのログイン要求が既にあった場合、同一のアカウントからのログイン要求があったことを示す同一ログインフラグをセットし(ステップS5)、既にログインしている会議出席者の有無を調べる(ステップS6)。会議出席者がいない場合、ステップS1の処理に戻って、次のログイン要求を待つ。一方、既に会議出席者がいる場合、正常にログインした出席者に不正なログインがあった旨の警告を送信する(ステップS7)。この後、ステップS1の処理に戻る。

【0068】そして、ステップS5で同一ログインフラグがセットされると、次にログイン要求があった場合、ステップS2における同一ログインフラグのチェックの結果、この会議には不正なログイン処理が行われている旨の警告を表示し(ステップS8)、ステップS1の処理に戻る。

【0069】そして、不正なログインがあると、MFAP5は、会議主催者だけにアクセスを許可する。不正なログインの警告を目にした会議主催者は、MFAP5に会議用設定情報の再発行を依頼する。依頼を受けたMFAP5は、会議用設定情報を新たに決定し、新たな設定用のファイルを着脱式記憶部54の記録媒体に書き込

む。この記録媒体には、新しい無線グループID、無線LAN用暗号化キー、この会議共通のアカウントおよびパスワードが記録されている。主催者は、この記録媒体を他の参加者に渡すか、あるいは無線LANの1対1通信モードを使用し、他の参加者に新しい会議用設定情報を通知する。不正ログインを行った第三者が、この時点で新たな会議用設定情報を知ることが不可能であるので、会議内容を知ることができない。MFAP5は、念のため、参加者のログイン数を調べ、予約時に登録されているメールアドレスの数とこのログイン数の比較を行う。

【0070】全ての出席者のログアウト処理が行われると、MFAP5は、会議終了と判断し、会議終了と判断した会議用のアカウントおよびパスワードを破棄する。さらに、無線LANアクセスポイント部52だけ電源を落とすか、MFAP5の全ての電源を落とし、不正なアクセスを防止する。

【0071】尚、電子メールそのものに、会議の日時、会議で使用する無線グループID、無線LAN用暗号化キー、1人分のアカウントおよび1人分のパスワードを記載する代わりに、電子メールにファイルを添付するようにしてもよい。この添付ファイルには、会議の日時、会議で使用する無線グループID、無線LAN用暗号化キー、1人分のアカウントおよび1人分のパスワードが記載されていればよく、同様の動作を実現可能である。

【0072】このように、第3の実施形態では、会議予約時に発行する電子メールに、会議の日時、会議で使用する無線グループID、無線LAN用暗号化キー、1人分のアカウントおよび1人分のパスワードを記載し、参加者が所有する端末に搭載されている会議システムにこれらの会議用設定情報を読み込ませるだけで、自動的に会議に参加でき、しかも、第三者による会議内容の盗聴といった悪意ある行為を防止できる。

【0073】〔第4の実施形態〕図9は第4の実施形態における電子会議システムの構成を示す図である。前記第1、第2および第3の実施形態と同一の構成要素については、同一の符号を付すことにする。図において、4は会議で使用する端末である。5は多機能アクセスポイントである。

【0074】多機能アクセスポイント5の内部構成は、図6に示す通り、前記第2の実施形態と同様である。すなわち、多機能アクセスポイント5は、制御部51、無線LANアクセスポイント部52、不揮発性記憶部53、着脱式記憶部54および有線LANインターフェイス55を有する。この無線LANアクセスポイント部52は、大人数での会議を行った場合、トラフィックの分散を図るために、複数存在する場合もある。

【0075】図10は第4の実施形態における会議の予約から会議開始までの処理手順を示すフローチャートである。多機能無線LANアクセスポイント(MFAP)

5は持ち運び自在であり、随時、有線LAN3に接続される。ここでは、会議予約時に有線LAN3に接続し、MFAP5で会議を予約する場合を示す。

【0076】MFAP5は、DHCPクライアント機能を有し、起動時に接続されている有線LAN3にネットワークアドレスが割り当てられるように、MFAP5に対し、DHCPサーバに関する設定を行うとともに、電子メールサーバに関する情報を設定しておく必要がある。

【0077】会議主催者は、MFAP5を有線LAN3に接続した状態で起動する。主催者は、MFAP5にログインして会議の予約を行う(S101)。予約の際、会議の日時および参加者のメールアドレスを登録する(S102)。会議の予約を受け付けると、MFAP5は、会議に必要な無線LANの無線グループIDおよび無線LAN用暗号化キーを決定し、さらに予約された会議だけで有効なアカウントおよびパスワードを参加者分だけ発行する(S201)。

【0078】登録されたメールアドレスを基に、これらの情報を電子メール内に記載し、各参加者に電子メールを送る(S202)。参加者宛ての電子メールには、会議の日時、会議で使用する無線グループID、無線LAN用暗号化キー、1人分のアカウントおよび1人分のパスワードが記載されている。尚、電子メールに記載されたこれらの会議用設定情報は、通常のテキストデータであってもよいが、会議システム(ソフトウェア)同士だけで有効な符号に置き換えておくことが望ましい。

【0079】MFAP5は、会議で使用する無線グループID、無線LAN用暗号化キー、全ての参加者のアカウント、およびこれらのアカウントに対応するパスワードを、MFAP5内部の不揮発性記憶部53に記録する。一連の予約受付が終了すると、MFAP5本体の表示部(図示せず)で表示するか、会議主催者に電子メールで予約受付終了を通知する(S206)。

【0080】MFAP5が、複数の無線LANアクセスポイント部52を有する場合、各々の無線LANアクセスポイント部52毎に異なる無線グループIDおよび無線LAN用暗号化キーを設定することで、会議時、MFAP5内の無線LANアクセスポイント部52に接続する端末4の数を均等化することができ、無線区間でのトラフィックの低下を防止することができる。この場合、内蔵する無線LANアクセスポイント52の数分だけ無線グループIDおよび無線LAN用暗号化キーを決定し、内蔵する無線LANアクセスポイント部52に、登録された会議参加者が均等になるように割り当てる(S201)。そして、登録されたメールアドレスを基に、これらの情報を電子メール内に記載し、各参加者に電子メールを送る(S202)。参加者宛ての電子メールには、会議の日時、MFAP5が割り当てた無線LANアクセスポイント部52の設定情報である無線グループI

Dおよび無線LAN用暗号化キー、および会議で使用する1人分のアカウントおよび1人分のパスワードが記載されている。

【0081】各会議参加者は、MFAP5から送られてきた電子メールを会議で使用する端末4に渡し、会議システムを起動させ、MFAP5から送られてきた電子メールを読み込ませる。会議システムは、読み込んだ電子メールから会議の日時、会議で使用する無線グループID、無線LAN用暗号化キー、1人分のアカウントおよび1人分のパスワードを取り出して記憶する。また、複数の会議を管理するために、図3に示す会議スケジュール管理を行う。会議参加者は、会議の日時および場所の情報だけを知ることができるが、会議の無線通信の設定情報やアカウントおよびパスワードについては、会議システムが管理するので、会議参加者は知らなくてもよい。また、第三者の目に触れさせないためにも、会議参加者の目に触れさせない方が望ましい。

【0082】会議主催者は、会議時、予約を行ったMFAP5を会議室に持ち込み、起動させる。MFAP5が起動すると、不揮発性記憶部53から会議用設定情報を読み込み、無線グループIDおよび無線LAN用暗号化キーを無線LANアクセスポイント部52に設定する(S207)。

【0083】参加者は、会議システムが搭載されている端末4を持ち込み、端末4を立ち上げ、会議システムを起動する。起動した会議システムは、予め読み込んだ電子メールに記載されていた会議で使用する無線グループIDおよび無線LAN用暗号化キーを、端末4に接続されている無線LANカードに設定する。端末4が無線LANを内蔵している場合、内蔵無線LANに設定する。

【0084】会議システムは、無線LANの接続を要求し(無線LAN認証要求、S103)、接続完了後(無線LAN認証確認、S104)、無線LANを経由して同じ電子メールに記載されていたアカウントでMFAP5内部の会議システムにログインし(ユーザ認証要求、S105)、パスワードで認証する(ユーザ認証確認、S106)。MFAP5は、不揮発性記憶部53に記憶されたアカウントおよびパスワードを参照し、有効なアカウント名である場合、会議に参加させる。

【0085】会議に代理人を出席させる場合、MFAP5から送られてきた電子メールを、電子メールで転送するか、あるいは記録媒体に記録して代理人に渡す。代理人は会議に持ち込む端末4に搭載されている会議システムを起動させ、MFAP5から送られてきた電子メールを会議システムに読み込ませる。出席者は変わっても、会議用のアカウントだけで有効な出席者であるか否かを判断するので、容易に代理人を出席させることが可能である。尚、同一のアカウントのログインが発生した場合の処理は、前記第3の実施形態と同様である。

【0086】そして、全ての出席者のログアウト処理が

行われると、MFAP5は、会議終了と判断し、会議終了と判断した会議用のアカウントおよびパスワードを破棄する。さらに、無線LANアクセスポイント部52だけ電源を落とすか、あるいはMFAP5の全ての電源を落として、不正なアクセスを防止する。

【0087】電子メールそのものに、会議の日時、会議で使用する無線グループID、無線LAN用暗号化キー、1人分のアカウントおよび1人分のパスワードを記載する代わりに、電子メールにファイルを添付してもよい、この添付ファイルには、会議の日時、会議で使用する無線グループID、無線LAN用暗号化キー、1人分のアカウントおよび1人分のパスワードが記載されていればよく、同様の動作を実現できる。

【0088】このように、会議予約時に発行する電子メールには、会議の日時、会議で使用する無線グループID、無線LAN用暗号化キー、1人分のアカウントおよび1人分のパスワードを記載し、参加者の端末に搭載されている会議システムに読み込ませるだけで、自動的に会議に参加でき、しかも、第三者による会議内容の盗聴するといった悪意ある行為を防止できる。

【0089】以上が本発明の実施の形態の説明であるが、本発明は、これら実施の形態の構成に限られるものではなく、特許請求の範囲で示した機能、または実施の形態の構成が持つ機能が達成できる構成であればどのようなものであっても適用可能である。

【0090】また、本発明は、前述した実施形態の機能を実現するソフトウェアのプログラムコードをシステムあるいは装置に供給することによって達成される場合、プログラムコード自体が本発明の新規な機能を実現することになり、そのプログラム自体およびそのプログラムを記憶した記憶媒体は本発明を構成することになる。このプログラムコードが格納される記憶媒体としては、ROM、フレキシブルディスク、ハードディスク、CD-ROM、CD-R、DVD、不揮発性のメモリカードなどを用いることができる。

【0091】

【発明の効果】本発明によれば、参加者が特別な作業を行うことなく会議に参加でき、しかも、第三者による会議内容の盗聴といった悪意ある行為を防止できる。

【図面の簡単な説明】

【図1】第1の実施形態における電子会議システムの構成を示す図である。

【図2】会議の予約から会議開始時までの動作処理手順を示すフローチャートである。

【図3】会議スケジュール管理を示す図である。

【図4】アカウントのログイン処理手順を示すフローチャートである。

【図5】第2の実施形態における電子会議システムの構成を示す図である。

【図6】多機能アクセスポイントの内部構成を示すプロ

ック図である。

【図7】第3の実施形態における電子会議システムの構成を示す図である。

【図8】第3の実施形態における会議の予約から会議開始時までの処理手順を示すフローチャートである。

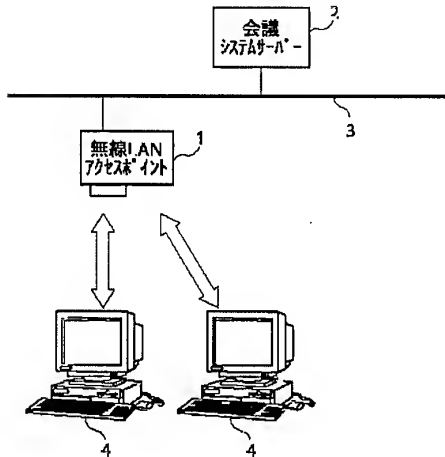
【図9】第4の実施形態における電子会議システムの構成を示す図である。

【図10】第4の実施形態における会議の予約から会議開始時までの処理手順を示すフローチャートである。

【符号の説明】

- 1 無線LANアクセスポイント
- 2 会議システムサーバ
- 3 有線LAN
- 4 端末
- 5 多機能アクセスポイント
- 6 会議予約サーバ
- 51 制御部
- 52 無線LANアクセスポイント部
- 53 不揮発性記憶部
- 54 着脱式記憶部

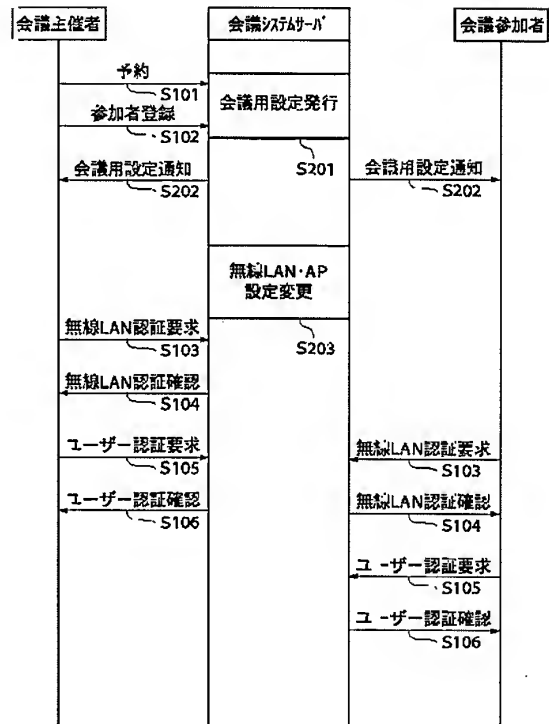
【図1】



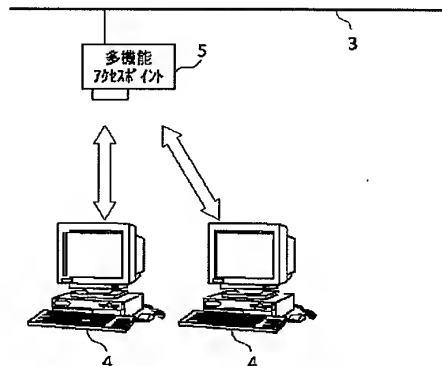
【図3】

ユーザーに見える情報	ユーザーに見えない情報
打ち合わせ ○月△日××時	ESSID: □○△× WEP: □□□× US: R: □□△× PASS: ××××
打ち合わせ ○月□日××時	ESSID: ○○○△ WEP: △△□□ US: R: ○○△□ PASS: ×○×○

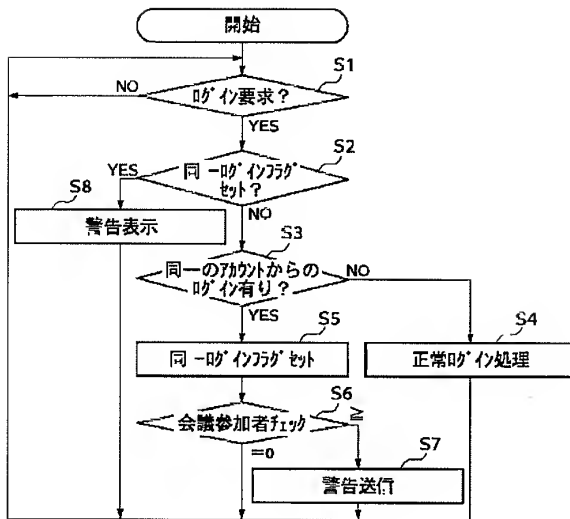
【図2】



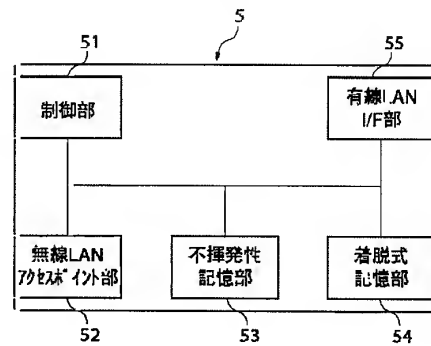
【図5】



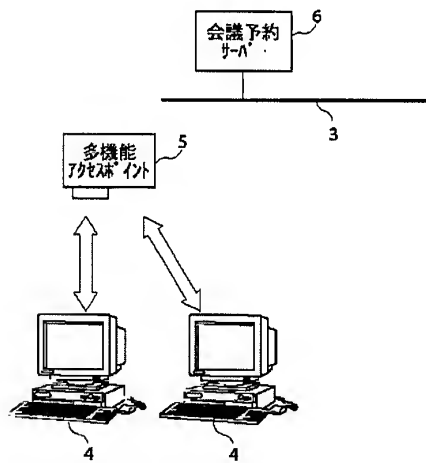
【図4】



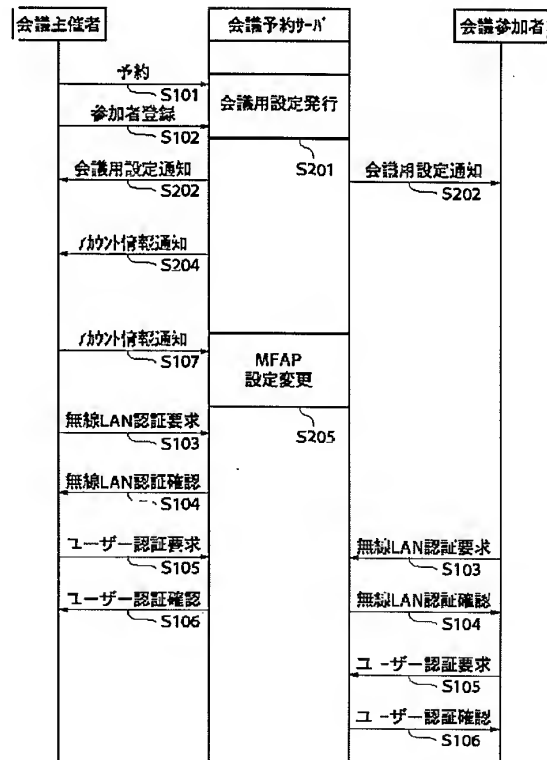
【図6】



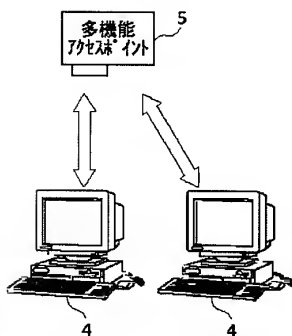
【図7】



【図8】



【図9】



【図10】

